Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Data Protection and Information Commissioner
FDPIC

Transborder data transfers briefly explained

For the attention of federal bodies and private industry

(Last modified: January 2017)

1) What is the aim of the revision of the Swiss Federal Data Protection Act (FADP) regarding transborder data transfers?

The revision is designed to adapt Swiss data protection to the Council of Europe Convention on the Protection of Individuals with regard to Automatic Processing of Personnel Data (Convention ETS 108).

This will result in:

- a comparable level of protection at the highest level possible, and unrestricted transborder data transfer between contracting states;
- a guarantee that the transfer of personal data to a data recipient who is not covered by the Convention will only be authorised if the recipient state or the recipient organisation can guarantee an appropriate level of protection.

2) Where and how are transborder data transfers regulated in the FADP?

The core provision which regulates transborder data transfers is Article 6 of the FADP. Other provisions in the FADP, together with the Ordinance to the Federal Act on Data Protection (OFADP) provide additional details as well as implementing regulations. It reads as follows:

[1] Personal data may not be transferred abroad if to do so might seriously jeopardise the personality rights of the data subject, in particular in cases when there is no legislation that can guarantee an appropriate level of protection.

[2] If there is no legislation that can guarantee an appropriate (sufficient) protection, personal data can only be transferred abroad, if:

a. sufficient guarantees are provided, particularly in the form of a contractual agreement, which certify an appropriate level of protection;

b. the data subject has given his or her consent;

c. the processing of the data is directly connected with the conclusion or performance of a contract, and the personal data are those of the contractual partner;

d. the disclosure of the data is essential in the specific circumstances, either as a result of an overwhelming public interest or for determining, exercising or enforcing legal rights before a court of law;

e. the disclosure is necessary in the specific circumstances in order to protect the life or physical integrity of the person concerned;

f. the data subject has made the data freely available and has not expressly forbidden their processing;

g. the disclosure takes place within the same legal entity or company, or between legal entities or companies which are run by the same management, to the extent that the persons concerned are covered by data protection rules which guarantee an appropriate level of protection..

level of protection, personal data may only be transferred abroad if:

[3] The Federal Data Protection and Information Commissioner, as defined in Article 26, must be kept informed about the level of guarantees provided in accordance with paragraph 2 a) and the data protection rules according to paragraph 2 g). The Federal Council shall specify the details of this duty to inform.

Feldeggweg 1, 3003 Bern
Tel. 058 462 43 95, Fax 058 465 99 96
www.edoeb.admin.ch

3) How has the wording of the new regulation changed?

The wording of the FADP has been adapted to the additional Protocol and the term “equivalent protection” has been replaced by “adequacy of protection”. In practice, however, this does not mean that the rules applicable to transborder data transfers have either been tightened or loosened.

4) Can the publication of personal data on the internet be considered as a transborder data transfer?

Using automated information and communication services, such as the internet, for the purposes of providing public information is not deemed to be a transborder data transfer (Art. 5 OFADP). All other data protection requirements remain valid. The Federal administration is bound in particular by the requirement that all data disclosure be covered by a legal basis. (Art. 19 FADP).

5) Grounds for a transborder data transfer:

Possible reasons for the transborder transfer of personal data might include:

- the need to centralize particular data processing operations;
- the outsourcing of data processing, or
- the take-over of a company by a foreign company.

6) What is meant by the duty of care on the part of the data controller who transfers data abroad, and are there different types of duty of care?

The duty of care means:

- respecting the general principles of data protection as defined in the FADP (general duty of care);
- guaranteeing the adequacy of data protection in the target country for each individual disclosure (special duty of care);
- informing the FDPIC in accordance with Art. 6 para. 3 of the FADP (special duty of care).

7) Which data protection principles must be respected under the general duty of care provision?

Private individuals which transfer personal data abroad must:

1. justify the data disclosure (Art. 13 para. 1 FADP). Acceptable grounds for disclosure include:
    a. the consent of the data subject(s),
    b. an overriding private or public interest, e.g. the centralisation of customer data or payroll accounting, or
    c. the existence of a legal basis.
2. verify the legality of the data transfer (Art. 4 para. 1 FADP). It is unlawful to disclose data if to do so constitutes an infringement of Swiss law.
3. make the planned data transfer known to the data subject in advance (principle of good faith, Art. 4 para. 2 and para. 4 FADP).
4. ensure the proportionality and appropriateness of the data transfer (Art. 4 para. 2 and 3 FADP). For example, if a company wants to centralise its payroll accounting abroad, only pay relevant data may be transferred, and they in turn may only be processed for the announced purpose.
5. guarantee the accuracy of the data (Art. 5 FADP).

6. take the appropriate technical and organisational measures to protect the integrity, confidentiality and availability of the data during the transfer (Art. 7 FADP).

8) Which data protection principles must be respected under the specific duty of care provision?

It is incumbent upon the data controller to:

- check the appropriateness of the protection in the target country (Art. 6 para. 1 FADP);
- respect alternative conditions in the event that the target country does not provide appropriate data protection (Art. 6 para. 2 FADP);
- notify the FDPIC in accordance with Art. 6 para. 3 FADP.

9) How should the appropriateness of protection in the target country in accordance with Art. 6 para. 1 FADP be assessed?

The data controller must verify that the principles set out in Convention ETS 108 and in the additional Protocol are reflected in both general and specific legal provisions, as well as in the legal practice of the host country. In particular, care must be taken to ensure

- *compliance with the principles of the FADP,*
- *the preservation of the data subject's interests in the event of non-compliance with such principles*
- *that the right to information is respected, and*
- *the existence of an independent supervisory body.*

With the implementation of the Swiss-US Privacy Shield, countries that guarantee an adequate level of data protection in terms of Art. 6 para. 1 Data Protection Act subject to certain requirements now include the USA. As under the Safe Harbor agreement, US companies which join Privacy Shield and which appear on the list issued by the US Department of Commerce (DOC) are deemed to offer an adequate level of protection in relation to personal data from Switzerland. In comparison with its predecessor framework, Privacy Shield brings stricter application of the data protection principles and closer supervision by the US authorities. Persons concerned are given specific instruments to enable them to find out directly from certified US companies or the competent authorities about data processing and to ensure that any required corrections or deletions are made. People can also indirectly influence the processing of their data by the US security services via an ombudsman procedure. FDPIC will act as a point of contact for persons in Switzerland in the event of any problems in connection with the transfer of data to the USA. A link to the list of all certified US companies and the other relevant documents will be provided here as soon as the certification process in the USA begins and the required information becomes available.

10) What role is played by the FDPIC's non-binding list of states that are deemed to have appropriate data protection legislation?

In order to ascertain compliance with the appropriateness principle, the data controller may rely on the list of states published by the FDPIC (Art. 31 para. 1 lit. d FADP and Art. 7 OFADP).

The list includes states which are

- contracting parties to Convention ETS 108 and the additional Protocol, or
- according to the FDPIC, provide an adequate level of data protection.

The list is kept constantly up to date and is not definitive. The fact that a country is not included on the list does not mean that it does not provide an adequate level of protection.

Furthermore, private individuals or federal bodies who transfer data to countries that are listed as providing «adequate protection» are assumed to have acted in good faith. However, if, on the basis of prior experience, they know that data protection principles in the recipient country are not respected either in general or in particular sectors, they may no longer claim to have acted in good faith. Under such circumstances disclosure may only take place under the terms of Art. 6 para. 2 FADP.

11) What is the purpose of Art. 6 para. 2 FADP?

If the protection provided by the law of the target country is not deemed to be appropriate, data may only be transferred if the conditions of Art. 6 para. 2 FADP are met.

Example: if the target country only provides an appropriate legal protection for data concerning natural persons, if the data concern legal entities, guarantees in accordance with Art. 6 para. 2 lit. a and g FADP must be provided. Even if no such guarantees can be provided, data may nevertheless be transferred to the country in question provided that the grounds set out under Art. 6 para. 2 lit b-f FADP are respected.

12) Under which contracts may data be transferred under the terms of Art. 6 para. 2 lit. a FADP?

The FDPIC has drawn up or recognised various standard contracts or standard contractual clauses (Art. 6 para. 3 OFADP) which include:

- The **standard contractual clauses of the European Union**:
- The **Council of Europe's model contract** for safeguarding an appropriate level of data protection in transborder data transfers
- The **FDPIC's model contract** for the outsourcing of data processing abroad

  NB.: In the case of outsourcing, the purpose of data processing remains the same for both the contracting authority and the contractor (cf. Art. 3 lit. i FADP). The contracting authority, moreover, remains the sole data controller, as it alone can determine the content and purpose of such data.

  Example: Payroll accounting is transferred to a contractor abroad.

  If it is not a case of outsourcing, the recipient of a data transfer usually replaces the original purpose of the processing with a new purpose. According to the FADP, he thus becomes the data controller.

  Example: Customer data which were originally intended exclusively for managing customer relations are then transferred and processed for marketing purposes.

Private persons or federal bodies that wish to transfer data may also apply other contractual agreements or guarantees. For example, they may decide to apply a specific data protection agreement or data protection clauses contained in other contracts. These clauses must guarantee an appropriate level of protection, i.e. one that is in conformity with the FADP. They must also cover all relevant aspects of the data transfer, in particular:

- the identity of the data transferor and the data recipient,
- the categories of data to be transferred,
- the purpose of the transfer,
- the categories of data subjects,
- the final data recipient and the amount of time the data will be kept.

Moreover, the data protection clauses must

- facilitate compliance with data protection principles
- safeguard the rights of data subjects, i.e. the right of access, rectification and opposition
- provide for a control mechanism
- include measures to safeguard safety and confidentiality during the transfer of particularly sensitive personal data or personality profiles.

13) Requirements for, and characteristics of, the consent applicable to transborder data transfers in accordance with Art. 6 para. 2 lit. b FADP:

The consent shall be:

- limited to individual cases, i.e. a specific situation. A blanket consent for the regular and systematic disclosure of data abroad for different purposes and in different situations is not permissible. In exceptional circumstances, the term “limited to individual cases” may cover not only a single transborder data transfer, but also an entire set of data transfers provided that the conditions remain the same (in particular with regard to purpose and recipient).

  Example: the transfer of several protocols from the same group, which includes persons from different countries, does not require their consent before each single document is transferred

- voluntary;
- accepted only after the data subject has been provided with the appropriate information (Art. 4 para. 5 FADP);
- explicit, if the disclosure concerns particularly sensitive personal data;
- liable to immediate withdrawal at any time for any future data processing or transfer.

Consent does not free the data controller from his duty of care, particularly with regard to the requirement that measures be taken to protect the data, or that compliance with the original purpose by the data recipient is verified.

14) What is meant by a data transfer for the conclusion or implementation of a contract according to Art. 6 para. 2 lit. c FADP?

A contractual partner transfers the personal data of another contractual partner to a third party abroad for the conclusion or performance of a contract.

Examples:

- A travel agency discloses customer data to a foreign hotel
- Data is disclosed to a credit information bureau in order to check creditworthiness within the framework of a sales contract
- A travel company discloses data to a transport company for the purpose of arranging international transportation (by rail, ship, airplane)
- Data are disclosed within the context of a bank transaction or an international payment order.

15) When and under what conditions may data be transferred according to Art. 6 para. 2 lit. d FADP?

The data transfer must:

- be justified by an overriding public interest or the requirements of legal proceedings
- be essential for the purpose of satisfying that interest,
- be rendered necessary by the specific case, i.e. only in a particular situation

Example:

For security reasons a football club transfers the personal data of hooligans to the country hosting the game.

However, the fact that a state invokes the fight against terrorism as a reason for requesting the data transfer, but actually intends to use the data for unlawful purposes, does not automatically satisfy the overriding interest requirement (e.g. for human rights abuses).

16) Under what conditions is a data transfer admissible according to Art. 6 para. 2 lit. e FADP?

According to this article, data may be transferred if:

- the vital interests of the data subject are affected,
- the data subject is not in a position to assert his or her own interests (e.g. as a consequence of an accident abroad),
- the approval of the person concerned by the data transfer can be assumed.

The data of persons who are close to the data subject may be transferred if the life of the latter is in danger and they cannot give their consent.

17) How can the transfer of generally available data be limited according to Art. 6 para. 2 lit. f FADP?

If a person has opened his or her own data to the public but does not wish that data to be liable to unrestricted processing, he or she must make it expressly known for what purposes the data may or may not be processed. Furthermore, it is conceivable that the data subject may inform a specific data processor that he or she does not want the public data concerning them to be processed (cf. Art. 12 para. 2 lit. b FADP).

18) What conditions must be met by internal company data protection rules according Art. 6 para. 2 lit. g FADP?

In order to ensure that company-wide data protection rules offset the lack of an appropriate level of data protection in the recipient country, they must meet the following conditions:

- Substantive provisions must be in place to ensure that at the very least they meet the requirements applicable to private data processors as set out in the European Convention on Data Protection ETS 108 and the additional Protocol (cf. the comments on Art. 6 para. 2 lit. a FADP).
- The rules applicable to the individual companies of a group must be formally binding and their practical application assured. The formal requirement, for example, can be addressed by a decision of the board of directors. As for their practical application, this can be assured, for example, by means of an audit.

Additional rules on data transfer according to Art. 6 para. 2 lit. g FADP:

- The data controller is not released from his responsibility to ensure that the data processing carried out in Switzerland complies with all the other provisions of the FADP.
- The individual companies belonging to a group must adopt and implement the rules.

19) When must the FDPIC be informed of a data transfer?

The duty to inform (Art. 6 para. 3 FADP and Art. 6 para. 1 OFADP) is applicable in the case of:

- data transfers according to Art. 6 para. 2 lit. a FADP (data protection covered by a contract)

- data transfers according to Art. 6 para. 2 lit. g FADP (data protection covered by internal company data protection rules).

20) How should the FDPIC be notified?

- The information should be provided in the form of a copy of the guarantees or data protection rules agreed with the recipient.
- If model agreements or standard contractual clauses are used, the data controller need only provide the FDPIC with general information about their use. If the data controller intends to apply other guarantees in particular circumstances or to particular parts of the data transfer, a copy of the contract must be sent to the FDPIC.
- The duty to inform is deemed to have been respected after the first notification for all further disclosures provided that they are covered by the same guarantees or data protection rules, and to the extent that the categories of recipients, the purpose of the processing and the data categories have not substantially changed.
- The FDPIC does not require information about each individual email or letter sent abroad. In particular, the duty to inform does not apply in the case of personal or private correspondence.
- The data controller must inform the FDPIC before the data are transferred abroad. Should this prove impossible, the information must be provided as soon as possible after the transfer.
- Information may be provided via the internet.
- The application forms used under the old FADP are no longer valid.
- Non-compliance with the duty to inform is a criminal offence (Art. 34 para. 2 lit. a FADP).

21) What does the examination of the FDPIC consist of?

- If recognised standard contracts are used for transborder data transfers, the FPIC will forego an examination of the applicable rules, and will confine himself to taking note of them.
- If a standard contract is not used, or if substantial aspects of such a standard contract have been modified, the FDPIC may decide to examine the rules. The FDPIC has 30 days within with to carry out his examination (Art. 6 para. 5 OFADP).
- If the guarantees and data protection rules are deemed not to provide an appropriate level of protection, the FDPIC may contact the data controller and, if appropriate, issue a recommendation in accordance with Art. 29 FADP.
- If there is no reaction from the FPDIC within the specified period, the data controller may assume that there are no objections to the guarantees and data protection rules that have been produced.

22) What are the consequences of infringing the duty of care provision?

The data controller is liable for all negative consequences arising from the infringement of his duty of care. In particular, he may be required to produce evidence showing that he has taken all necessary measures to safeguard an adequate level of protection. The Ordinance further refines this aspect of the duty of care since it requires the data controller to take appropriate measures to ensure that the recipient complies with the data protection guarantees or rules (Art. 6 para. 4 OFADP).

23) Can the data subject sue in the event of an infringement of the duty of care?

The data subject can sue in a court of law if data are transferred abroad in breach of the duty of care in accordance with Art. 15 para. 1 FADP.

24) According to Art. 11a FADP, must data files be notified if personal data are regularly transferred to third parties abroad?

Yes, according to Art. 11a para. 3 lit. b FADP, data files must be notified to the FDPIC. The purpose of notification is to ensure the transparency of all data files that are regularly transferred abroad.

The requirement to provide information to the FPDIC about the transborder data transfer remains unaffected by this provision in accordance with Art. 6 para. 3 FADP.